

Exhibit No. 8

June 2005



Highlights of GAO-GAO-05-677, a report to congressional requesters

TRANSPORTATION SECURITY ADMINISTRATION

Clear Policies and Oversight Needed for Designation of Sensitive Security Information

Why GAO Did This Study

Concerns have arisen about whether the Transportation Security Administration (TSA) is applying the Sensitive Security Information (SSI) designation consistently and appropriately. SSI is one category of "sensitive but unclassified" information—information generally restricted from public disclosure but that is not classified. GAO determined (1) TSA's SSI designation and removal procedures, (2) TSA's internal control procedures in place to ensure that it consistently complies with laws and regulations governing the SSI process and oversight thereof, and (3) TSA's training to its staff that designate SSI.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct TSA to establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI; establish clear responsibility for the identification and designation of SSI information; establish internal controls monitoring compliance with its SSI regulations, policies, and procedures, and communicate that responsibility for implementing the controls throughout TSA; and provide specialized training to those making SSI designations on how information is to be identified and evaluated for SSI status. The Department of Homeland Security generally concurred with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-05-677.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Laurie E. Ekstrand at (202) 512-8777 or ekstrandl@gao.gov.

What GAO Found

TSA does not have guidance and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI or who can make the designation. Such guidance is required under GAO's standards for internal controls. In addition, TSA has no policies on accounting for or tracking documents designated as SSI. As a result, TSA was unable to determine either the number of TSA employees actually designating information as SSI or the number of documents designated SSI. Further, apart from Freedom of Information Act (FOIA) requests or other requests for disclosure outside of TSA, there are no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed.

TSA also lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA. Specifically, TSA has not established and documented policies and internal control procedures for monitoring compliance with the regulations, policies, and procedures governing its SSI designation process, including ongoing monitoring of the process. TSA officials told us that its new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. This office, which was established in February 2005, will also develop and implement all TSA policy concerning SSI handling, training, and protection. More detailed information on how this office's activities will be operationalized was not yet available. Specifically, TSA officials provided no written policies formalizing the office's role, responsibilities, and authority.

TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is identified and evaluated for protected status. Development of such training for SSI designations is needed to help ensure consistent implementation of the designation authority across TSA. While TSA has provided a training briefing on SSI regulations to certain staff, such as the FOIA staff, it does not have specialized training in place to instruct employees on how to consistently designate information as SSI. In addition, TSA has no written policies identifying who is responsible for ensuring that employees comply with SSI training requirements.



United States Government Accountability Office
Washington, DC 20548

June 29, 2005

The Honorable David Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives

The Honorable Martin Olav Sabo
Ranking Minority Member
Subcommittee on Homeland Security
Committee on Appropriations
House of Representatives

The security of our transportation system is of vital importance to the nation. In line with keeping our transportation safe, some information that is related to threats to or protection of the transportation system must be held out of the public domain. On the other hand, the government must always be mindful of the public's legitimate interest in, and need to know, information related to threats to the transportation system and associated vulnerabilities.

Sensitive Security Information (SSI) is a specific category of information related to transportation security that is deemed to require protection against public disclosure. Although it is not classified national security information, SSI is a category of sensitive but unclassified information that, along with protected critical infrastructure information, is specifically exempted by statute from release under the Freedom of Information Act (FOIA), and that it is to be disclosed only to covered persons on a need to know basis. While the Transportation Security Administration (TSA), through its SSI authority, may share SSI with regulated entities, it generally prohibits the public disclosure of information obtained or developed in the conduct of security activities, which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential commercial or financial information, or be detrimental to the security of transportation.

Questions have been raised about TSA's practices and procedures for determining whether information should be protected as SSI. For example, certain written responses to questions submitted by TSA to the House Appropriations Homeland Security Subcommittee were designated as SSI. However, 1 month earlier, the agency had not treated this same

information as sensitive. Further, in an October 2004 memorandum, TSA itself recognized that the handling and identification of SSI had become problematic.

In response to your request concerning TSA's handling of SSI, we are reporting on (1) TSA's procedures for determining whether information should be protected under the SSI designation, as well as procedures for determining if and when the designation should be removed, (2) internal control procedures in place to ensure that TSA consistently complies with laws and regulations governing the designation of information as SSI and how TSA oversees the procedures to ensure that they are consistently applied, and (3) TSA's training to its staff who designate SSI.

To address our objectives, we reviewed applicable federal laws and regulations, Department of Homeland Security (DHS) and TSA policies and procedures, and other documents related to the SSI designation, and oversight and training processes. We also interviewed TSA and DHS officials involved in the SSI designation, oversight and training processes. GAO's *Standards for Internal Control in the Federal Government* provided benchmarks and standards against which we assessed TSA's SSI designation policies and procedures.¹ Our work was conducted from January 2005 through April 2005 in accordance with generally accepted government auditing standards.

On April 29, 2005, we provided your offices a briefing on the results of our work. The briefing slides are included in appendix I.

Background

In the aftermath of the terrorist attacks of September 11, 2001, TSA was created to take responsibility for the security of all modes of public transportation. Included in the responsibilities of this new agency was the authority to designate information as SSI. Originally housed in the Department of Transportation, TSA was transferred to DHS as a result of the Homeland Security Act of 2002.²

¹GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

²The Homeland Security Act of 2002 established 49 U.S.C. § 114(s) as TSA's SSI authority. TSA codified its SSI regulations at 49 C.F.R. part 1520.

According to TSA officials, SSI designated information is created by TSA and by airports, aircraft operators, and other regulated parties when they are establishing or implementing security programs or documentation to address security requirements. Information that is designated SSI can be shared with those who have a need to know in order to participate in or oversee the protection of the nation's transportation system. Those with a need to know can include persons outside of TSA, such as airport operators, aircraft operators, foreign vessel owners, and other persons. SSI cannot be shared with the general public, and it is exempt from disclosure under FOIA.

There are 16 categories of SSI. TSA has distinguished these 16 categories into 3 types of SSI. Four categories are termed "categorical" and automatically designated SSI. Eleven categories require a judgment or analysis to determine if the SSI designation is warranted. One category requires a written determination by an office with determination authority to be deemed SSI. This category is "other information," which is a catchall exemption for information that TSA may wish to designate SSI that does not fit into the other 15 categories.³

Additional background information on the SSI regulatory authority, including a list of the 16 categories, is included in appendix I.

Results

TSA does not have written policies and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI. Written guidance for decision making such as this is a key element included in GAO's *Standards for Internal Control in the Federal Government*. Lack of such guidance could result in errors and inconsistencies in determining the SSI designation. Indeed, in October 2004, TSA's Internal Security Policy Board concluded that TSA must establish a framework to identify, control, and protect SSI. The board concluded that essential elements of the framework should include, among other things,

"... exacting specificity with respect to what information is covered and what is not covered. This specificity could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining SSI. Experience

³A subset of one of the judgment categories, 49 C.F.R. § 1520.5(9)(iii), also falls within this determination category.

has shown that employees unsure as to what constitutes SSI may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure.”

In addition to lacking written guidance concerning SSI designation, TSA has no policies and procedures specifying clear responsibilities for officials who can designate SSI.⁴ TSA’s regulations allow anyone within TSA to designate information SSI. Further, TSA has no policies on accounting for or tracking documents designated as SSI. While TSA officials told us that only a limited number of employees routinely make SSI designations, they were unable to provide documentation to confirm this. One consequence of a lack of control of personnel able to designate documents as SSI is that TSA is unable to determine the number of employees designating information as SSI or the volume of documents designated SSI.

Once a document is designated SSI, it can remain designated as SSI in perpetuity unless a FOIA request or other request for disclosure outside of TSA results in removal of its SSI status. If a FOIA request is received for an SSI designated document, or a document that contains some SSI designated material, the SSI Program Office works in conjunction with the FOIA Office to review its initial designation. If TSA officials determine that the document should no longer be considered SSI, it can be released to the FOIA requester. If TSA officials feel that the SSI designation should remain but some portions of the document are not SSI, the FOIA Office can determine whether it is appropriate to release the document without the SSI material, or not to release the document at all.⁵ Other than the FOIA process, no procedures exist for the review of allegations that a document has been erroneously designated as SSI. If there is no FOIA request for a particular document, according to TSA, documents marked as SSI are reviewed for continued applicability upon any request for disclosure outside of TSA. However, TSA officials provided us with no information

⁴TSA identified two categories of information—§§ 1520.5(b)(9)(iii) and 1520.5(b)(16)—that require a written determination by an office with determination authority to be designated SSI.

⁵ According to a TSA official, TSA processed 99 FOIA requests involving or related to SSI in 2003 and 129 requests in 2004. The TSA official said that, of the total requests processed in 2003, no requests were granted in whole, 63 requests were granted in part, and 36 requests were denied in full. The official also said that, of those 129 requests processed in 2004, no requests were granted in whole, 92 requests were granted in part, and 37 requests were denied in full.

on the number of documents released as a result of these requests for public disclosure. TSA's SSI regulations indicate that TSA may determine in writing that information should no longer be designated as SSI because it no longer meets SSI criteria, but TSA has not done this to date.

TSA lacks adequate internal controls to provide reasonable assurance that its SSI designation process is being consistently applied across TSA and for monitoring compliance with the regulations governing the SSI designation process, including ongoing monitoring of the process. GAO's Standards for Internal Control call for (1) areas of authority and responsibility to be clearly defined and appropriate lines of reporting established, (2) transactions and other significant events to be documented clearly and documentation to be readily available for examination, and (3) controls generally to be designed to ensure that ongoing monitoring occurs in the course of normal operations. In addition, the standards also require that information be communicated within an organization to enable individuals to carry out their internal control responsibilities. However, our review of TSA's oversight activities noted weaknesses in each of these areas.

First, TSA has not clearly defined responsibility for monitoring compliance with regulations, policies and procedures governing the SSI designation process and communicated that responsibility throughout TSA. Without clearly identifying the responsibility for monitoring compliance with regulations governing its SSI designation, this function may not receive adequate attention, leaving TSA unable to provide reasonable assurance that those making SSI designations within TSA are designating documents properly.

In an October 14, 2004, memorandum designed to centralize the administration of SSI within the agency, TSA's Internal Security Policy Board recognized that the handling and identification of SSI had become problematic:

"Lacking a central policy program office for SSI has led to confusion and unnecessary classification of some materials as SSI. Adherence to handling requirements within TSA has been inconsistent, and there have been instances where SSI has been mishandled outside of TSA. Identification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending on the viewpoint, experience, and training of the identifier. Strictures on the release of SSI and other SSI policy or handling-related problems have occasionally frustrated industry stakeholders, Congress, the media, and our own employees trying to work within the confines of the restrictions. Significant time and effort

has been devoted to SSI issues, and it is not likely that the current approach to addressing such issues can be sustained.”

TSA officials told us that its new SSI Program Office will ultimately be responsible for ensuring that staff are consistently applying SSI designations. This office, which was established in February 2005, will also develop and implement all TSA policies concerning SSI handling, training, and protection. Officials said that TSA is also currently drafting a summary that provides a definition and brief overview of the SSI authority and is designing materials that will further educate all TSA employees on policies, procedures, responsibilities, and guidance for identifying and designating SSI. More detailed information on how this office’s activities will be operationalized was not yet available. Specifically, TSA currently does not have written policies formalizing the office’s role, responsibilities, and authority.

Second, TSA has not yet established policies and procedures for how it will monitor compliance with the regulations governing the SSI designation process. Without written policies and procedures documenting how it plans to monitor compliance with the regulations governing the SSI designation process, TSA is unable to demonstrate evidence of its monitoring activities.

Third, TSA has no formally defined policies or procedures for ongoing monitoring reviews to assess compliance with the laws and regulations governing the process for designating information as SSI. Without clearly defined policies and procedures for conducting periodic internal monitoring to assess compliance with the regulations governing the SSI designation process, TSA lacks structure to support continuous assurance that those employees making SSI designations within TSA are designating documents properly.

TSA has not developed policies and procedures for providing specialized training for all of its employees making SSI designations on how information is to be identified and evaluated for protected status. Development of specialized training for SSI designations must be preceded by the establishment of guidance and associated policies and procedures so that an adequate training curriculum can be developed. It should also include written policies defining who is responsible for ensuring that employees comply with SSI training requirements. While TSA has provided a training briefing on SSI regulations to certain staff such as the FOIA staff and other units within TSA, it does not have specialized training in place to instruct employees on how to consistently designate information as SSI.

Conclusions

In order for TSA's SSI designation process to work effectively, there must be clarity, structure, and accountability to help ensure that information is not improperly and unnecessarily restricted or inappropriately disclosed, and that the SSI designation process is being applied consistently across TSA. The lack of clear and documented policies and procedures for determining what constitutes SSI and specifying who may make the designation could cause confusion and uncertainty for staff who must administer the SSI designation process without written guidance. Further, internal control policies and procedures for monitoring the compliance with regulations governing the SSI designation process, including internal controls for ongoing monitoring, communicated to all staff, would help ensure accountability and consistency in the implementation of TSA's SSI regulations. Specialized training designed to familiarize those who are making SSI designations on how information is to be identified and evaluated would reduce the likelihood that employees improperly exempt information from public disclosure or inappropriately disclose sensitive security information.

Recommendations

To help bring clarity, structure, and accountability to TSA's SSI designation process, we recommend that the Secretary of the Department of Homeland Security direct the Administrator of the Transportation Security Administration to take the following four actions

- establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI,
- establish clear responsibility for the identification and designation of information that warrants SSI protection,
- establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA, and
- establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status.

Agency Comments and Our Evaluation

We obtained written comments on a draft of this report from the Department of Homeland Security. We have included a copy of the

comments in their entirety in appendix II. In addition, DHS provided technical comments, which we incorporated as appropriate.

In its June 14, 2005, comments, DHS generally concurred with our recommendations and stated that they are consistent with ongoing TSA efforts to improve sensitive security information program processes. In its comments, DHS discussed the actions it has already taken and will implement in response to the recommendations, including developing internal controls and audit functions, which will define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process, and which will be communicated throughout TSA. However, as discussed below, DHS took exception to the report's analyses and conclusions. While we disagree with the thrust of DHS's comments, we believe we fairly and accurately characterize the implementation and monitoring of SSI at DHS. We made clarifying changes where appropriate.

DHS said that our report mischaracterized the nature of SSI by incorrectly applying concepts associated with classified information management to SSI information, which falls within a sensitive but unclassified information category. DHS said that this construct may lead the reader to fundamental misunderstandings regarding the issues surrounding SSI. Although mentioned as a basis for comparison, neither the GAO review nor its report was intended to apply concepts associated with classified information management to SSI. Rather, our analyses were intended to provide a factual summary of the key similarities and differences in the classified information and SSI processes. We compare the two processes only to help clarify the distinctions that exist and thereby avoid any misunderstandings by readers who are familiar with the processes for classified information. We included additional language in the report clarifying that SSI is a form of sensitive but unclassified information, rather than classified national security information.

DHS also stated that SSI is the only practical means for sharing security information with regulated parties and that the absence of a robust SSI program would degrade both the prompt distribution of security information to persons with a need to know and the free exchange of ideas. We agree that SSI is a practical means for sharing security information with regulated parties. In fact, the findings and recommendations in this report should help DHS improve the SSI process. That is, providing specific procedures and guidelines on how individual employees are to identify and evaluate information for SSI protected status is an intrinsic part of DHS's responsibility for effectively managing

its SSI process and should provide both DHS and the regulated parties with confidence that information is given the proper protective status.

DHS said that if a TSA employee incorrectly designates a document as SSI while it remains within TSA, there is no impact on the public's right to access because the FOIA review process will always result in an independent determination regarding the SSI designation and that TSA and DHS are committed to releasing as much information as possible. We view the management improvements discussed in this report as helping to ensure that information that should be withheld from the public is protected as well as helping to ensure that other information is available to the public. In addition, the fact that an incorrectly designated SSI document remains within TSA does not obviate the fact it is wrongfully exempted from disclosure. The potential lack of visibility to the public that SSI documents exist and the time and expense to the public and TSA involved in seeking disclosure of an SSI document through FOIA could inhibit the release of information that could and possibly should have been in the public domain but for an incorrect application of SSI.

DHS also states that we make no distinction between the obligation to "mark" information as SSI, held by all TSA employees, and the authority to "designate," held by only a very few high-level employees. It explains that all employees can "mark" documents that fall within 15 categories as SSI but only the high-level employees can "designate" the 16th category of "other information" by documenting the designation as SSI. As we point out in this report, the responsibility of all TSA employees goes beyond just marking a document as SSI and includes making judgments about what information should be marked as SSI. As we state on page 3, while TSA requires a written determination by an office with determination authority for information deemed SSI for 1 of its 16 SSI categories, according to TSA, only 4 of the remaining 15 categories automatically becomes SSI because of the type of document. The other 11 require a judgment or analysis to be made to determine if the SSI designation is warranted by any TSA employee. Therefore, we continue to believe that appropriate guidance and controls are needed to effectively manage the process.

In addition, DHS said that its SSI designation processes are consistent with every sensitive but unclassified system in the federal government. While we did not review these other systems, we believe that the management principles and controls discussed in this report are appropriate for the TSA system and would be appropriate for similar systems elsewhere.

DHS said that we made an implied suggestion to quantify and identify all documents that have been marked as SSI, and to identify all personnel who have marked such documents. We did note in our discussion of internal controls that TSA has no policies on accounting for or tracking documents designated as SSI. As DHS notes, we did not recommend that TSA provide an inventory of the titles or numbers of SSI documents. In terms of identifying staff that designate documents as SSI, since we are recommending training for all those who designate SSI, identification of all personnel who are going to be applying this designation would be needed to ensure that all are trained.

Further, DHS states that we obliquely criticize TSA's ability to protect SSI without a date by which the document automatically loses its SSI status based on time duration requirements similar to those applicable to classified information. We did not recommend that TSA should implement time limits for SSI information. Our review showed that TSA has no written policies and procedures or systematic reviews for determining if and when an SSI designation should be removed. Moreover, other than the FOIA request process and other requests for disclosure outside of TSA, no procedures exist for a review to determine whether a document has been appropriately designated as SSI. Such procedures would allow TSA to periodically review SSI designations and identify and correct erroneously marked SSI documents while still protecting those with valid reasons.

In commenting on our recommendation that DHS establish clear guidance and procedures for using the TSA regulations to determine what constitutes SSI, DHS said that TSA's SSI Program Office has already taken some steps in line with our recommendation by developing internal guidance that expands on the SSI regulation structure to provide examples of the types of information that should fall within each SSI category. It expects to publish the guidance for general use by TSA employees and regulated parties in identifying and handling SSI.

In commenting on our recommendation that DHS establish clear responsibility for the identification and designation of information that warrants SSI protection, DHS stated that limiting the number of individuals who may designate a document as SSI would lead to operational bottlenecks, could lead to inappropriate release of security information, and would not be operationally feasible. If it is properly done, we do not see how establishing clear responsibility for performing a governmental task would lead to these effects. We wish to make a distinction between a set of personnel who would have responsibility for SSI and a potentially much larger set of employees who would be able to

designate documents SSI. Those responsible for SSI would be accountable for ensuring that those in their domain of responsibility have appropriate training and are applying SSI appropriately. DHS would then be in a much better position to ensure that those responsible for SSI are held accountable, have appropriate training, and are applying SSI appropriately.

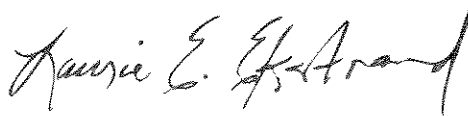
DHS agreed with our recommendation for DHS to establish internal controls that clearly define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and communicate that responsibility throughout TSA. DHS said it had already undertaken action to develop internal controls, including audit functions, which will define responsibility for monitoring compliance with regulations, policies, and procedures governing the SSI designation process and will communicate that responsibility throughout TSA.

In commenting on our recommendation that DHS establish policies and procedures within TSA for providing specialized training to those making SSI designations on how information is to be identified and evaluated for protected status, DHS said that it conducts specialized SSI training for the SSI Program Office and FOIA staff, and other TSA offices making SSI designations. In addition, it is expanding specialized training to those offices within the agency that create the majority of SSI. This is a good first step in addressing our recommendation, but falls short of its overall intent because SSI regulations extend the SSI designation authority to all TSA employees and does so without giving them specific procedures and guidance, beyond the regulations, upon which to base their judgments. Thus, policies and procedures for providing specialized training to all TSA employees authorized to make an SSI designation will still be needed. In this regard, in our report, we quote an October 14, 2004, TSA memorandum that says in part, "identification of SSI has often appeared to be ad-hoc, marked by confusion and disagreement depending on the viewpoint, experience, and training of the identifier." We believe this statement speaks to the need for specialized training for all those who designate materials as SSI.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to other interested congressional committees and to the Secretary of the Department of Homeland Security and the Administrator of the Transportation Security Administration. We will also make copies

available to others upon request. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or EkstrandL@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Glenn G. Davis, Vickie Miller, R. Rochelle Burns, Julian King, Thomas Lombardi, David Hooper, David Plocher, Dolores McGhee, Nikki Clowers, Kim Gianopoulos, David D'Agostino, Ann Borseth, William Cawood, Casey Keplinger, David Alexander, Katherine Davis, and Larry Harrell.



Laurie E. Ekstrand, Director
Homeland Security and Justice Issues